

09/20/00
JCS U. S. PTO

09-21-00

A

Please type a plus sign (+) inside this box → PTO/SB/05 (1/98)
Approved for use through 09/30/2000. OMB 0551-0032
Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

**UTILITY
PATENT APPLICATION
TRANSMITTAL**

(Only for new nonprovisional applications under 37 CFR 1.53(b))

Attorney Docket No. 042390.P8184

First Inventor or Application Identifier Luke E. Girard, et al.

Title Method and Apparatus to Improve the Protection...

Express Mail Label No. EL485757315US

APPLICATION ELEMENTS
See MPEP chapter 600 concerning utility patent application contents.

1. Fee Transmittal Form (e.g., PTO/SB/17)
(Submit an original, and a duplicate for fee processing)
2. Specification [Total Pages 18]
(preferred arrangement set forth below)
 - Descriptive title of the Invention
 - Cross References to Related Applications
 - Statement Regarding Fed sponsored R & D
 - Reference to Microfiche Appendix
 - Background of the Invention
 - Brief Summary of the Invention
 - Brief Description of the Drawings (if filed)
 - Detailed Description
 - Claim(s)
 - Abstract of the Disclosure
3. Drawing(s) (35 U.S.C. 113) [Total Sheets 5]
4. Oath or Declaration [Total Pages 5]
 - a. Newly executed (original or copy)
 - b. Copy from a prior application (37 C.F.R. § 1.63(d))
(for continuation/divisional with Box 17 completed)
(Note Box 5 below)
 - i. DELETION OF INVENTOR(S)
Signed statement attached deleting inventor(s) named in the prior application, see 37 C.F.R. §§ 1.63(d)(2) and 1.33(b).
5. Incorporation By Reference (useable if Box 4b is checked)
The entire disclosure of the prior application, from which a copy of the oath or declaration is supplied under Box 4b, is considered to be part of the disclosure of the accompanying application and is hereby incorporated by reference therein

ADDRESS TO: Assistant Commissioner for Patents
Box Patent Application
Washington, DC 20231

6. Microfiche Computer Program (Appendix)
7. Nucleotide and/or Amino Acid Sequence Submission
(if applicable, all necessary)
 - a. Computer Readable Copy
 - b. Paper Copy (identical to computer copy)
 - c. Statement verifying identity of above copies

ACCOMPANYING APPLICATION PARTS

8. Assignment Papers (cover sheet & document(s))
9. 37 C.F.R. §3.73(b) Statement
(when there is an assignee) Power of Attorney
10. English Translation Document (if applicable)
11. Information Disclosure Statement (IDS)/PTO-1449 Copies of IDS Citations
12. Preliminary Amendment
13. Return Receipt Postcard (MPEP 503)
(Should be specifically itemized)
14. Small Entity Statement(s) Statement filed in prior application, Status still proper and desired (PTO/SB/09-12)
15. Certified Copy of Priority Document(s)
(if foreign priority is claimed)
16. Other:

* A new statement is required to be entitled to pay small entity fees, except where one has been filed in a prior application and is being relied upon.

17. If a CONTINUING APPLICATION, check appropriate box, and supply the requisite information below and in a preliminary amendment:

Continuation Divisional Continuation-in-part (CIP)

of prior application No: /

Prior application information: Examiner _____ Group / Art Unit: _____

18. CORRESPONDENCE ADDRESS

Customer Number or Bar Code Label or Correspondence address below
(Insert Customer No. or Attach bar code label here)

Name	John Travis				
Address	Blakely, Sokoloff, Taylor & Zafman				
City	Los Angeles	State	CA	Zip Code	90025-1026
Country	USA	Telephone	512-330-0844	Fax	512-330-0476

Name (Print/Type)	John Travis	Registration No. (Attorney/Agent)	43,203
Signature	<i>John Travis</i>	Date	9-20-00

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Box Patent Application, Washington, DC 20231.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

FEE TRANSMITTAL

for FY 2000

Patent fees are subject to annual revision.
 Small Entity payment must be supported by a small entity statement, otherwise large entity fees must be paid. See Forms PTO/SB/09-12. See 37 C.F.R. §§ 1.27 and 1.28.

TOTAL AMOUNT OF PAYMENT (\$ 844.00)

Complete if Known

Application Number	Not assigned
Filing Date	Herewith
First Named Inventor	Luke E. Girard, et al.
Examiner Name	Not assigned
Group / Art Unit	Not assigned
Attorney Docket No.	042390.P8184

METHOD OF PAYMENT (check one)

The Commissioner is hereby authorized to charge indicated fees and credit any overpayments to:

Deposit Account Number 02-2666

Deposit Account Name Blakely, Sokoloff, Taylor & Zafman

Charge Any Additional Fee Required
Under 37 CFR §§ 1.16 and 1.17

Payment Enclosed:

Check Money Order Other

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Small Entity Fee Code (\$)	Fee Code (\$)	Fee Code (\$)	Fee Description	Fee Paid	
105 130	205	65	Surcharge - late filing fee or oath		
127 50	227	25	Surcharge - late provisional filing fee or cover sheet		
139 130	139	130	Non-English specification		
147 2,520	147	2,520	For filing a request for reexamination		
112 920*	112	920*	Requesting publication of SIR prior to Examiner action		
113 1,840*	113	1,840*	Requesting publication of SIR after Examiner action		
115 110	215	55	Extension for reply within first month		
116 380	216	190	Extension for reply within second month		
117 870	217	435	Extension for reply within third month		
118 1,360	218	680	Extension for reply within fourth month		
128 1,850	228	925	Extension for reply within fifth month		
119 300	219	150	Notice of Appeal		
120 300	220	150	Filing a brief in support of an appeal		
121 260	221	130	Request for oral hearing		
138 1,510	138	1,510	Petition to institute a public use proceeding		
140 110	240	55	Petition to revive - unallowable		
141 1,210	241	605	Petition to revive - unintentional		
142 1,210	242	605	Utility issue fee (or reissue)		
143 430	243	215	Design issue fee		
144 580	244	290	Plant issue fee		
122 130	122	130	Petitions to the Commissioner		
123 50	123	50	Petitions related to provisional applications		
126 240	126	240	Submission of Information Disclosure Stmt		
581 40	581	40	Recording each patent assignment per property (times number of properties)		
146 690	246	345	Filing a submission after final rejection (37 CFR § 1.129(a))		
149 690	249	345	For each additional invention to be examined (37 CFR § 1.129(b))		
Other fee (specify) _____					
Other fee (specify) _____					
SUBTOTAL (2)	(\$)	114.00	SUBTOTAL (3)	(\$)	40.

* Reduced by Basic Filing Fee Paid

SUBTOTAL (3) (\$ 40.

SUBMITTED BY

Name (Print/Type)	John F. Travis	Registration No. (Attorney/Agent)	43,203	Telephone	512/330-0844
Signature	John F. Travis			Date	9-20-00

WARNING:

Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

Burden Hour Statement: This form is estimated to take 0.2 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

UNITED STATES PATENT APPLICATION

for

**METHOD AND APPARATUS TO IMPROVE THE PROTECTION OF
INFORMATION PRESENTED BY A COMPUTER**

Inventors:

Luke E. Girard
Steven G. Preston
Daniel J. Lenehan

Prepared by:

Blakely, Sokoloff, Taylor & Zafman
12400 Wilshire Boulevard
Seventh Floor
Los Angeles, California
(512) 330-0844

Docket No.: 042390.P8184

EXPRESS MAIL CERTIFICATE OF MAILING

"Express Mail" mailing label number EL485757315US Date of Deposit September 20, 2000

I hereby certify that I am causing this paper or fee to be deposited with the United States Postal Service "Express Mail Post Office to Addressee" service on the date indicated above and that this paper or fee has been addressed to the Assistant Commissioner for Patents, Washington, D. C. 20231.

Shenise Ramdeen
(Typed or printed name of person mailing paper or fee)

Shenise Ramdeen
(Signature of person mailing paper or fee)

METHOD AND APPARATUS TO IMPROVE THE PROTECTION OF INFORMATION PRESENTED BY A COMPUTER

5

BACKGROUND OF THE INVENTION

1. Field of the Invention

The invention pertains generally to computer security. In particular, it pertains to protecting electronic documents on a computer from unauthorized copying or other
10 harmful intervention.

2. Description of the Related Art

Widespread use of the Internet and email has left millions of personal
15 computers (PCs) vulnerable to downloaded viruses and other types of malicious
software that can destroy programs, copy and upload private documents, and perform
other harmful acts, frequently without the PC operator's knowledge. The increasing
popularity of downloaded programs has multiplied the problem significantly, since it
creates so many more opportunities to unknowingly download the malicious software.
Due to their open architecture, most PCs provide very little protection against such
20 destructive software. It is this very openness that has made the PC platform the
general-purpose solution provider that it is. Other types of computers are also
vulnerable to such attacks in varying degrees, but the pervasive use of PCs has drawn
much attention to the problem as it applies to PCs.

In the past, owners of copyrighted information or other intellectual property
25 have been reluctant to allow their property to be viewed on the PC platform (books,
movies, sensitive corporate documents, etc.) as the nature of the open PC platform
makes the property vulnerable to mischievous software that may be running in parallel.

Although self-replicating destructive software (viruses) attracts the most attention, copyright owners are more concerned with the illegal copying and distribution of any document that they permit to be downloaded to a computer. This is particularly true of e-books, or books that are available electronically by downloading the text of those 5 books over a network such as the Internet. The ease of copying documents downloaded into a PC makes it easy to illicitly reproduce and forward copyrighted materials without detection of this activity by the copyright owner.

Fig. 1 shows a conventional system 10. Protected content in the form of encrypted data is provided over channel 11 to storage subsystem 12, where it is stored 10 for subsequent use. Channel 11 could be an Internet connection and the portion of a PC that receives and processes network data. Storage subsystem 12 could be main memory, the hard disk on the PC, or some other form of storage. When the data is ready for presentation, it can be retrieved from storage 12 and presented to player 14 for processing. Player 14 is generally software running in the PC. Decryption of the 15 encrypted data can take place in player 14, which can also reformat the data. The processed data can then be passed over channel 15 to graphics sub-system 16, where it is formatted for presentation over channel 17 to the actual display device, such as a video monitor. Note: although the terms "document" and "display" are used here, this scenario applies equally well to graphics video data and to audio data, such as music, 20 that is played through speakers.

Fig. 2 shows a conventional graphics controller 16. Previous attempts to protect downloaded data have focused primarily on encrypting the data for delivery and storage. However, once the data is decrypted, formatted, and sent to the graphics controller 16 through primary interface 21, the bit-image of that data is generally placed 25 in a video memory 22 where the data is repeatedly read out and transmitted through

output port 23 to a display device. For reasons of flexibility and usability, the contents of video memory 16 can generally be read through primary interface 21 by the PC that implements player 14, and may be read by other devices as well through that same interface. Many graphics controllers also have a secondary interface 24 that also
5 permits both read and write capability of video memory 22 by other devices, as well as permitting direct transmission of video data to output port 23 when that capability is needed. Output port 23 generally does not provide memory read capability. However, interfaces 21 and 24 provide two ports through which the data in video memory 22 can be captured, and subsequently saved and/or transmitted, for later display in an
10 unauthorized manner. For efficiency of transmission, the offending software that captures the bit-image from video memory can also use the text font maps stored in the PC to interpret the bit image and convert any displayable text back to a standard word processing format. Thus, by using resources freely available in the PC, the supposedly protected data in graphics controller 16 can not only be retrieved and stored and/or
15 transmitted to another device, but the retrieved data can be reverse-engineered into a much more compact and usable form before such storage/transmission.

Since many players are in the form of a PC that is vulnerable to modification by maliciously loaded software, this exposure of the graphics subsystem creates a security problem that discourages the use of PCs for any displayable data that needs to be
20 protected, such as copyrighted video material. Once the data is placed in graphics subsystem 16, that data is vulnerable to unauthorized monitoring and capture by software that has been illicitly placed in the computer.

It is not only downloaded malicious software that can compromise the security
25 of the data. The PC operator might wish to illicitly copy the data, which he or she legitimately downloaded, for subsequent illicit use or distribution.

SUMMARY OF THE INVENTION

An embodiment of the invention includes a method that includes receiving data
5 in a presentation buffer of a presentation controller, and receiving a request from a
requestor to read the data in the presentation buffer. It further includes deleting the data
from the presentation buffer in response to the request and not delivering the data to the
requestor in response to the request.

10

BRIEF DESCRIPTION OF THE DRAWINGS

15

Fig. 1 shows a prior art system.

Fig. 2 shows a prior art graphics controller.

Fig. 3 shows a graphics controller of the invention.

Fig. 4 shows a control circuit of the invention.

Fig. 5 shows a system of the invention.

20

DETAILED DESCRIPTION OF THE INVENTION

When electronic documents are downloaded from a publisher/owner to a
computer for display, unauthorized copying, diversion, modification, destruction, or
other harmful effects to that data can take place at several points. The data needs to be
25 protected from those harmful effects during delivery to the player, inside the player,

outside the player, and at the display. This invention focuses on protecting the data in the graphics subsystem, and can include elements in the player to implement that protection.

Fig. 3 shows a graphics controller 30 of the invention. Rendered data from the player can be received through primary interface 31 for subsequent storage in video memory 32. Memory 32 includes a frame buffer for storing the portion of the stored image that is actually displayed. Data from the frame buffer can then be sent to an output interface 33, which sends a properly formatted signal to the display device. Output interface 33 can include a random access memory digital-to-analog converter (RAMDAC), which converts the digitized data into one or more properly formatted analog signals with the specified color rendition. Other types of display devices might require a different output interface to format the data in a different manner, but the overall process within graphics controller 30 is basically the same. A secondary interface 34 can also provide a secondary port to a data channel 18 for data destined for video memory 32, or provide video data directly to output interface 33. Unlike a conventional graphics controller, however, graphics controller 30 can contain a control circuit 35 to monitor and/or control data flowing between video memory 32 and either of interfaces 31 or 34, and to control video memory 32 in a manner that protects secure data stored therein from being illicitly read by devices external to graphics controller 30. Thus control circuit 35 can act as a gatekeeper between video memory 32 and devices external to graphics controller 30.

The operation of control circuit 35 can be broken down into several functional areas: mode control, security setup, security violation detection, response to violation, and termination. These are described in more detail below:

Mode Control

Control circuit 35 (and therefore graphics controller 30) can have two modes: a security mode and a by-pass mode. In the by-pass mode, the security features of control circuit 35 are by-passed, and graphics controller 30 can effectively perform as a conventional graphics controller. In the security mode, control circuit 35 can perform security functions to prevent all or a portion of the contents of video memory 32 from being read through interface 31. If interface 34 has a read capability, control circuit 35 can also be coupled to interface 34 to prevent video memory 32 from being read through interface 34. The mode can be established by one or more commands from the computer controlling circuit 35. In one embodiment, mode commands, other commands, associated addresses and video data can all be input through interface 31 along with other commands and data to be written to video memory. In another embodiment, commands and addresses can be input through one or more separate interfaces (not shown). In one embodiment, the security mode can be entered simply with an external command, but the security mode can be exited only if the secure data is deleted first. This prevents illicit software from simply turning off the security mode so that the protected data can be read with impunity.

20 Security Setup

The display device in a conventional system frequently shows multiple windows at the same time, some of them overlapping others. Thus the frame buffer may contain multiple windows, or portions of windows, at any given time. Since all the displayed windows are in the frame buffer, and the frame buffer can be read by

external devices in a conventional system, the displayed contents of any window are freely accessible to external devices in a conventional system.

When a copyrighted document or other secure data is being displayed, the window containing that secure data may be only one of several windows that are being
5 simultaneously shown on various parts of the display device. Several of those windows may contain non-secure data that the operator wishes to handle in a standard manner. For example, while viewing portions of a secure copyrighted e-book in one window, the operator may wish to read e-mail or look up an appointment notebook in another window, without having to exit from the e-book application. Therefore the protected
10 portion of the data may be only a subset of the frame buffer, and the secure portion of the data should be defined separately from the remaining displayed data.

The invention can define the coordinates of a secure window within the frame buffer. These coordinates can be contained in a set of registers that define opposite corners of a rectangular displayed window, such as the upper left and lower right
15 corners of that window. Any data that is located within this window is considered secure, and can be protected. In one embodiment, one or more sets of registers are dedicated to defining secure windows in this manner. In another embodiment, existing registers that define a window are temporarily designated as secure registers as long as the defined window contains secure data, but those registers can return to non-secure
20 status once the secure data is automatically deleted and/or the window is closed. In both embodiments, multiple sets of registers can be used to define multiple secure windows, so that the security function can be performed simultaneously on different windows. Note: although the term 'registers' is used here, the invention can also use other forms of data storage to hold the coordinates of the secure windows, such a block

of memory containing multiple memory locations. Such obvious design tradeoffs are within the capability of an average circuit designer.

Security registers can be loaded with the coordinates of the secure window by appropriate setup commands passed through interface 31. This assumes interface 31
5 supports conveyance of a combination of commands and data. Alternately, setup commands can be passed to control circuit 35 through another interface (not shown) specially designated for this purpose. In one embodiment, once these setup commands are entered, the designated security coordinates cannot be altered without deleting the protected data defined by these coordinates. This protects against malicious software
10 that accesses the secure data simply by changing the coordinates of the protected area to another location.

Security Violation Detection

Regardless of the register configuration used, the data within the secure window
15 can be treated as write-only data for all devices other than output circuit 33 which, by necessity, must read the contents of video memory so that it can display the image on a display device. All other devices, i.e., devices that can read video memory through interfaces 31, 34, or any other accessory ports, are prevented from reading any data in the window defined by the contents of the secure registers. Data in the frame buffer
20 that is outside this defined security window can be read in the normal manner. This effectively prevents the pre-defined secure data in the frame buffer from being illicitly read, copied, or transmitted by malicious software, while not interfering with normal operations for the rest of the data in the frame buffer.

Detection of an attempted security violation can be accomplished by monitoring
25 the addresses of any requests to read data from video memory 32. If the requested

address falls between the two stored addresses that define the opposite corners of a protected window, then a violation has occurred. When multiple security windows are defined at the same time, a separate comparison can be made for each secure window. A violation of any secure window can trigger a response.

5

Response to Violation

The no-read function can be enforced in various ways. In one embodiment, when a device attempts to read data from the secure area defined by the security registers, a data protector in graphics controller 30 will return video data, but not the requested video data. The controller might return a solid color for all of the locations in the protected area (such as blue, black, white, etc.). The controller might also return random data, resulting in an image of static. Another option is to return a window with an warning message, alerting the operator to the fact that protected data has been requested.

A second embodiment provides greater protection. In this embodiment, any attempt to read data from the protected portion of video memory can result in purging the protected portion of the data by the data protector. This can be done by overwriting the protected data with other data, such as the solid color, random data, or error message described above. This step can be followed by exiting the secure mode, so that the requested window is available for reading, but the secure data is no longer in it. These actions can also trigger other defensive mechanisms, such alerting the operator, deleting the other secure data that is still stored in encrypted form on disk, or severing the connection to the remote source of the secure data. Such drastic actions can prevent alternate, repeated attacks on the secure data by removing the secure data from the system altogether.

Some computer systems, such as laptop PCs, provide an external connector on the graphics controller so that other display devices can be attached. Besides the previously described features, additional protection can be provided by disabling the external graphics connector when secure data is being displayed so that external equipment can't just record the signal.

Termination

When the need to display protected data is over, commands can be issued to control circuit 35 to delete the secure window and/or to change the mode of the affected window from security to by-pass. In either case, the protected data within that window can be purged from video memory first so that it cannot be subsequently read by external devices. One or more commands can be implemented that terminate the secure mode in this manner. Alternately, termination can be triggered by simply attempting a read of the protected data, thereby artificially forcing a termination in the manner described above under 'Response to Violation'.

Fig. 4 shows a view of an embodiment of control circuit 35 in more detail. Fig. 4 is intended to show functional relationships rather than circuit connections, although a circuit can be modeled after the figure. Commands, addresses, and data can be received from interface 31 by circuit 41. Although Fig. 4 shows all commands, addresses, and data entering circuit 41 through a common port, different input ports and circuits can also be provided to handle commands and data separately. Logic 41 can also be divided into separate sections (not shown), a command handler for handling commands and/or the associated addresses, and another for handling video data to/from video memory. After receipt from interface 31, video data can be passed by data handling logic in circuit 41 along data path 40 en route to video memory 32. Read data

requested from video memory 32 can also travel in the opposite direction along bi-directional data path 40 and be provided to the requestor when such read data transactions are permitted.

Command handling logic in circuit 41 can decode mode or setup commands 5 input into circuit 35. A security mode command can cause line 49 to be set, thereby enabling mode enable gate 46. This in turn enables the security mode, so that any subsequent commands and data will be processed according to the security requirements. Command handling logic in circuit 41 can also accept the upper left and lower right coordinates of a secure window, placing them into upper-left address 10 register 44 and lower-right address register 45, respectively. These can be security registers dedicated to the security function, or can be existing registers that are temporarily designated as security registers. Subsequently, when a read command is received, command decode logic 41 can place the requested read address in register 42, where it can be compared with the two coordinate addresses in registers 44, 45. If the 15 address in the read command falls between the upper-left and lower-right addresses, inclusively, address compare logic 43 can set the line to mode enable gate 46, which can act as a security violation detector. If the other input of mode enable gate 46 is already set (because the circuit is in security mode) then gate 46 can activate the line to data protector 47, triggering a series of steps that respond to the detected security 20 violation by deleting the secure data in the frame buffer and possibly disabling the security mode.

Fig. 5 shows a system 50 of the invention. Protected content from a provider can be input through channel 11 and stored in storage medium 12, as in the prior art. The data for presentation can then be passed to player 54, which has the capability to 25 implement the aforementioned security features in graphics controller 30. Channels 55

and 57 can pass the video data to graphics controller 30 and the display, respectively.

The invention can be implemented in circuitry or as a method. The functional steps in the previous paragraphs can be performed with dedicated logic, a state machine, a processor, or any combination of these. The invention can also be 5 implemented as instructions stored on a machine-readable medium, which can be read and executed by at least one processor to perform the functions described herein. A machine-readable medium includes any mechanism for storing or transmitting information in a form readable by a machine (e.g., a computer). For example, a machine-readable medium can include read only memory (ROM); random access 10 memory (RAM); magnetic disk storage media; optical storage media; flash memory devices; electrical, optical, acoustical or other form of propagated signals (e.g., carrier waves, infrared signals, digital signals, etc.), and others.

The invention has been described in terms of a frame buffer in a video controller. However, it may be applied to other forms of data presentation. The video 15 controller may be generalized as a presentation controller, which can also take the form of an audio controller that presents downloaded audio information such as music or spoken words. The frame buffer may be generalized as a presentation buffer, which can also take the form of an audio buffer that temporarily stores the audio data to be played, including a combination of protected and non-protected audio data. An 20 embodiment of the invention using audio data can be used to play music or to present an audible e-book for the vision-impaired.

The foregoing description is intended to be illustrative and not limiting. Variations will occur to those of skill in the art. Those variations are intended to be included in the invention, which is limited only by the spirit and scope of the appended 25 claims.

We claim:

1 1. A method, comprising:
2 receiving data in a presentation buffer of a presentation controller;
3 receiving a request from a requestor to read the data in the presentation buffer;
4 deleting the data from the presentation buffer in response to the request; and
5 not delivering the data to the requestor in response to the request.

1 2. The method of claim 1, wherein the presentation controller is a graphics
2 controller and the presentation buffer is a frame buffer.

1 3. The method of claim 1, wherein receiving data includes placing the presentation
2 controller in a security mode.

1 4. The method of claim 1, wherein deleting the data includes taking the
2 presentation controller out of the security mode.

1 5. The method of claim 1, wherein not delivering the data includes delivering data
2 other than the data requested.

1 6. A machine-readable medium having stored thereon instructions, which when
2 executed by at least one processor cause said at least one processor to perform:
3 receiving data in a presentation buffer of a presentation controller;
4 receiving a request from a requestor to read the data in the presentation buffer;
5 deleting the data from the presentation buffer in response to the request; and

6 not delivering the data to the requestor in response to the request.

1 7. The medium of claim 6, wherein the presentation controller is a graphics
2 controller and the presentation buffer is a frame buffer.

1 8. The medium of claim 6, wherein receiving data includes placing the
2 presentation controller in a security mode.

1 9. The medium of claim 6, wherein deleting the data includes taking the
2 presentation controller out of the security mode.

1 10. The medium of claim 6, wherein not delivering the data includes delivering data
2 other than the data requested.

1 11. An apparatus, comprising:
2 a presentation controller having:
3 a presentation buffer;
4 a command handler to process commands and addresses;
5 a data handler coupled to the presentation buffer to monitor data and to
6 pass at least a part of the data to the presentation buffer;
7 a security violation detector to detect a request by a requestor to read
8 protected data in the presentation buffer; and
9 a data protector coupled to the data handler to prevent providing the
10 protected data to the requestor.

1 12. The apparatus of claim 11, wherein the data protector is further to purge the
2 protected data from the presentation buffer upon detection of the request to read
3 protected data.

1 13. The apparatus of claim 11, wherein the presentation controller is a graphics
2 controller and the presentation buffer is a frame buffer.

1 14. The apparatus of claim 11, wherein the presentation controller includes a by-
2 pass mode that does not prevent providing the protected data to the requestor.

1 15. The apparatus of claim 14, wherein the data protector:
2 is to purge the protected data from the presentation buffer upon detection of the
3 request to read protected data; and
4 is to place the presentation controller in the by-pass mode after said purge.

1 16. The apparatus of claim 11, wherein the data protector is to deliver data other
2 than the data requested.

1 17. A system, comprising:
2 a presentation circuit including:
3 an input interface to receive data;
4 an output port to transmit data for presentation;
5 a presentation buffer coupled to the output port;
6 a presentation controller coupled to the presentation buffer and to the
7 input interface and having:

8 a command handler to process commands and addresses; and
9 a data handler to monitor data and to pass at least a part of the
10 data to the presentation buffer;
11 a security violation detector to detect a request by a requestor to
12 read protected data in the presentation buffer; and
13 a data protector to prevent providing the protected data to the
14 requestor.

1 18. The system of claim 17, wherein the data protector is further to purge the
2 protected data from the presentation buffer upon detection of the request to read
3 protected data.

1 19. The system of claim 17, wherein the presentation controller is a graphics
2 controller and the presentation buffer is a frame buffer.

1 20. The system of claim 17, wherein the presentation controller includes a by-pass
2 mode that does not prevent providing the protected data to the requestor.

1 21. The system of claim 20, wherein the data protector:
2 is to purge the protected data from the presentation buffer upon detection of the
3 request to read protected data; and
4 is to place the presentation controller in the by-pass mode after said purge.

1 22. The system of claim 17, wherein the data protector is to deliver data other than
2 the data requested.

ABSTRACT OF THE DISCLOSURE

An improvement to a graphics controller to prevent the contents of selected portions of the frame buffer from being read by devices external to the graphics controller. The invention defines one or more viewable rectangles in the frame buffer as a protected write-only area. Any attempt to read data from the protected area of the frame buffer triggers a security violation which can delete or destroy the contents of that area to prevent it from being read. The controller can also operate in a bypass mode in which the security functions are bypassed so the graphics controller operates in a conventional manner. A security violation may return the controller to the bypass mode. The invention can prevent protected data, such as copyrighted data downloaded over the Internet, from being copied from the frame buffer and used in an unauthorized manner.

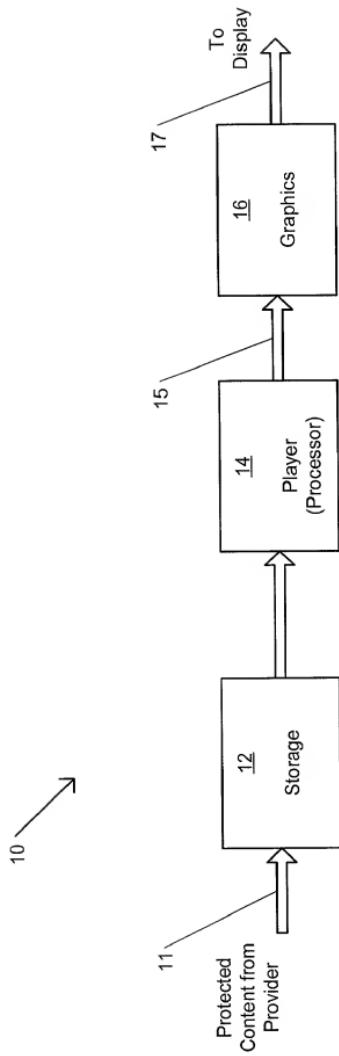


Fig. 1 Prior Art

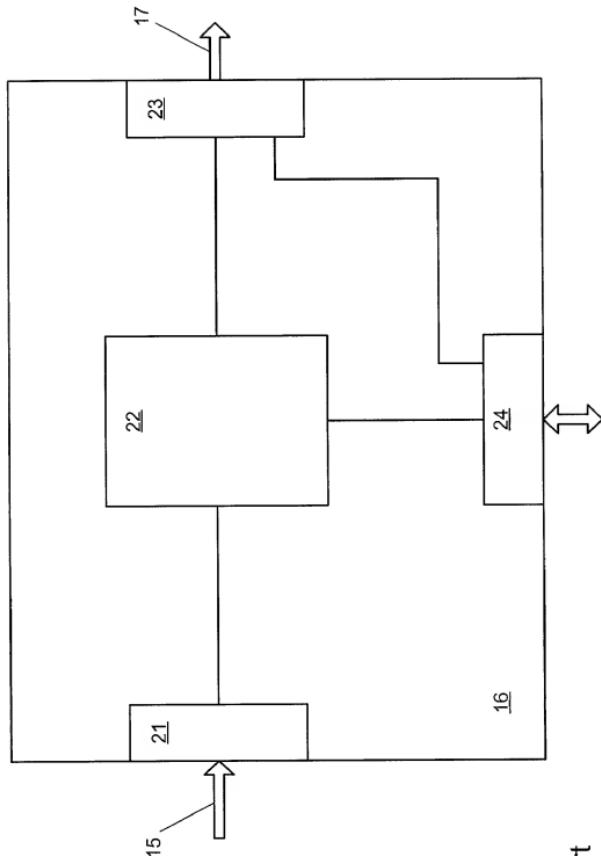


Fig. 2

Prior Art

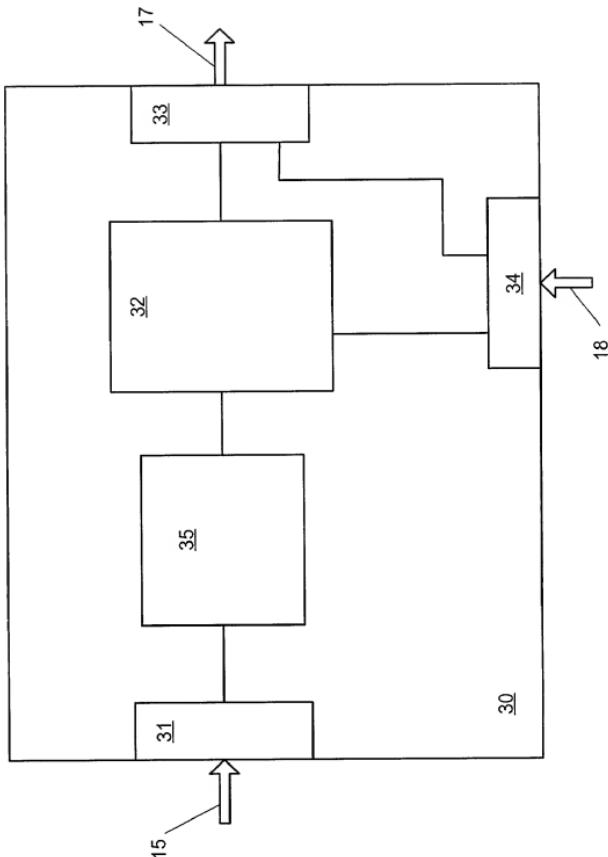


Fig. 3

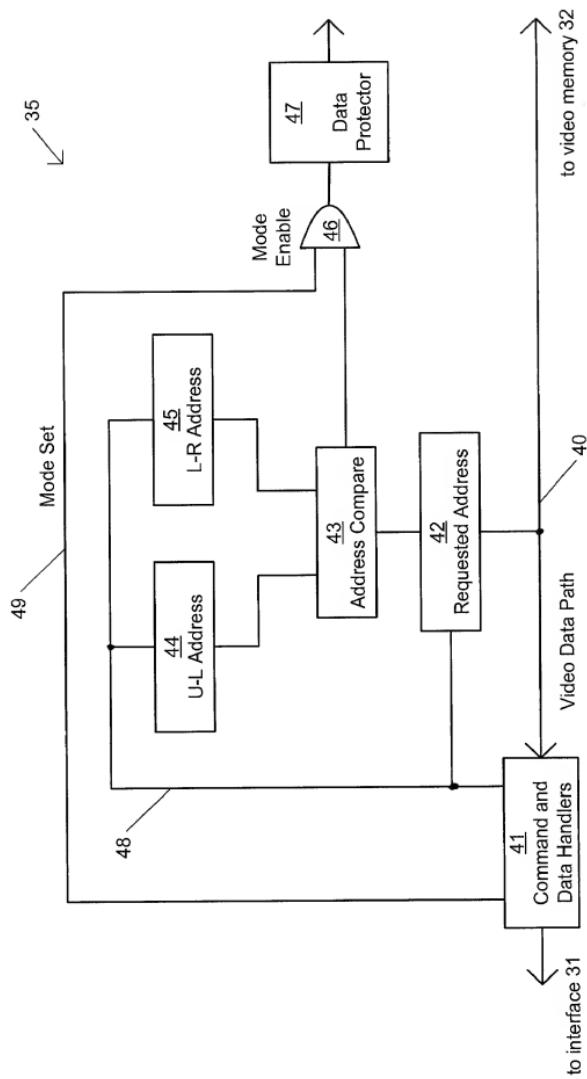


Fig. 4

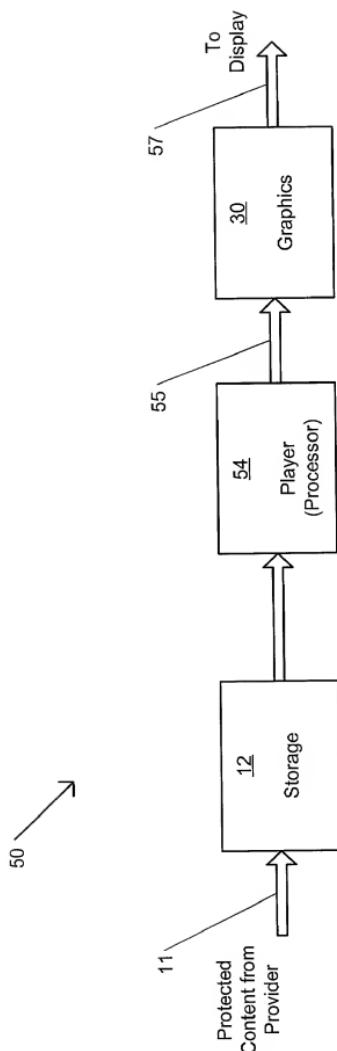


Fig. 5

DECLARATION AND POWER OF ATTORNEY FOR PATENT APPLICATION
(FOR INTEL CORPORATION PATENT APPLICATIONS)

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below, next to my name.

I believe I am the original, first, and sole inventor (if only one name is listed below) or an original, first, and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

**METHOD AND APPARATUS TO IMPROVE THE PROTECTION
OF INFORMATION PRESENTED BY A COMPUTER**

the specification of which

X is attached hereto.
— was filed on _____ as
United States Application Number _____
or PCT International Application Number _____
and was amended on _____
(if applicable)

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claim(s), as amended by any amendment referred to above. I do not know and do not believe that the claimed invention was ever known or used in the United States of America before my invention thereof, or patented or described in any printed publication in any country before my invention thereof or more than one year prior to this application, that the same was not in public use or on sale in the United States of America more than one year prior to this application, and that the invention has not been patented or made the subject of an inventor's certificate issued before the date of this application in any country foreign to the United States of America on an application filed by me or my legal representatives or assigns more than twelve months (for a utility patent application) or six months (for a design patent application) prior to this application.

I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56.

I hereby claim foreign priority benefits under Title 35, United States Code, Section 119(a)-(d), of any foreign application(s) for patent or inventor's certificate listed below and have also identified below any foreign application for patent or inventor's certificate having a filing date before that of the application on which priority is claimed:

<u>Prior Foreign Application(s)</u>	<u>Priority Claimed</u>
-------------------------------------	-----------------------------

(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No
(Number)	(Country)	(Day/Month/Year Filed)	Yes	No

I hereby claim the benefit under Title 35, United States Code, Section 119(e) of any United States provisional application(s) listed below:

<u>Application Number</u>	<u>Filing Date</u>
<u>Application Number</u>	<u>Filing Date</u>

I hereby claim the benefit under Title 35, United States Code, Section 120 of any United States application(s) listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States application in the manner provided by the first paragraph of Title 35, United States Code, Section 112, I acknowledge the duty to disclose all information known to me to be material to patentability as defined in Title 37, Code of Federal Regulations, Section 1.56 which became available between the filing date of the prior application and the national or PCT international filing date of this application:

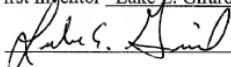
<u>Application Number</u>	<u>Filing Date</u>	<u>Status -- patented, pending, abandoned</u>
<u>Application Number</u>	<u>Filing Date</u>	<u>Status -- patented, pending, abandoned</u>

I hereby appoint the persons listed on Appendix A hereto (which is incorporated by reference and a part of this document) as my respective patent attorneys and patent agents, with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

Send correspondence to John Travis, Reg. No. 43,203, BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, 12400 Wilshire Boulevard 7th Floor, Los Angeles, California 90025 and direct telephone calls to John Travis, Reg. No. 43,203, (512) 330-0844.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

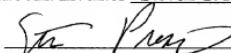
Full Name of Sole/First Inventor Luke E. Girard

Inventor's Signature  Date 9/6/2000

Residence Santa Clara, California Citizenship USA
(City, State) (Country)

Post Office Address 239 Rodonovan Court
Santa Clara, California 95051

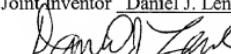
Full Name of Second/Joint Inventor Steven G. Preston

Inventor's Signature  Date 12 Sept 2000

Residence San Jose, California Citizenship USA
(City, State) (Country)

Post Office Address 346 Gordon Avenue
San Jose, California 95127

Full Name of Third/Joint Inventor Daniel J. Lenehan

Inventor's Signature  Date 9/1/00

Residence Los Altos Hills, California Citizenship USA
(City, State) (Country)

Post Office Address 24183 Dawn Ridge Drive
Los Altos Hills, California 94024

APPENDIX A

William E. Alford, Reg. No. 37,764; Farzad E. Amini, Reg. No. P42,261; Aloysius T. C. AuYeung, Reg. No. 35,432; William Thomas Babbitt, Reg. No. 39,591; Carol F. Barry, Reg. No. 41,600; Jordan Michael Becker, Reg. No. 39,602; Bradley J. Bereznak, Reg. No. 33,474; Michael A. Bernadicou, Reg. No. 35,934; Roger W. Blakely, Jr., Reg. No. 25,831; Gregory D. Caldwell, Reg. No. 39,926; Ronald C. Card, Reg. No. P44,587; Thomas M. Coester, Reg. No. 39,637; Stephen M. De Clerk, under 37 C.F.R. § 10.9(b); Michael Anthony DeSanctis, Reg. No. 39,957; Daniel M. De Vos, Reg. No. 37,813; Robert Andrew Diehl, Reg. No. 40,992; Matthew C. Fagan, Reg. No. 37,542; Tarek N. Fahmi, Reg. No. 41,402; James Y. Go, Reg. No. 40,621; James A. Henry, Reg. No. 41,064; Willmore F. Holbrow III, Reg. No. P41,845; Sheryl Sue Holloway, Reg. No. 37,850; George W Hoover II, Reg. No. 32,992; Eric S. Hyman, Reg. No. 30,139; Dag H. Johansen, Reg. No. 36,172; William W. Kidd, Reg. No. 31,772; Erica W. Kuo, Reg. No. 42,775; Michael J. Mallie, Reg. No. 36,591; Andre L. Marais, under 37 C.F.R. § 10.9(b); Paul A. Mendonsa, Reg. No. 42,879; Darren J. Milliken, Reg. 42,004; Lisa A. Norris, Reg. No. P44,976; Chun M. Ng, Reg. No. 36,878; Thien T. Nguyen, Reg. No. 43,835; Thinh V. Nguyen, Reg. No. 42,034; Dennis A. Nicholls, Reg. No. 42,036; Daniel E. Ovancezian, Reg. No. 41,236; Babak Redjaian, Reg. No. 42,096; William F. Ryann, Reg. 44,313; James H. Salter, Reg. No. 35,668; William W. Schaal, Reg. No. 39,018; James C. Scheller, Reg. No. 31,195; Jeffrey Sam Smith, Reg. No. 39,377; Maria McCormack Sobrino, Reg. No. 31,639; Stanley W. Sokoloff, Reg. No. 25,128; Judith A. Szepesi, Reg. No. 39,393; Vincent P. Tassinari, Reg. No. 42,179; Edwin H. Taylor, Reg. No. 25,129; John F. Travis, Reg. No. 43,203; George G. C. Tseng, Reg. No. 41,355; Joseph A. Twarowski, Reg. No. 42,191; Lester J. Vincent, Reg. No. 31,460; Glenn E. Von Tersch, Reg. No. 41,364; John Patrick Ward, Reg. No. 40,216; Charles T. J. Weigell, Reg. No. 43,398; Kirk D. Williams, Reg. No. 42,229; James M. Wu, Reg. No. P45,241; Steven D. Yates, Reg. No. 42,242; and Norman Zafman, Reg. No. 26,250; my patent attorneys, and Andrew C. Chen, Reg. No. 43,544; Justin M. Dillon, Reg. No. 42,486; Paramita Ghosh, Reg. No. 42,806; and Sang Hui Kim, Reg. No. 40,450; my patent agents, of BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP, with offices located at 12400 Wilshire Boulevard, 7th Floor, Los Angeles, California 90025, telephone (310) 207-3800, and Alan K. Aldous, Reg. No. 31,905; Robert D. Anderson, Reg. No. 33,826; Joseph R. Bond, Reg. No. 36,458; Richard C. Calderwood, Reg. No. 35,468; Jeffrey S. Draeger, Reg. No. 41,000; Cynthia Thomas Faatz, Reg. No. 39,973; Sean Fitzgerald, Reg. No. 32,027; Seth Z. Kalson, Reg. No. 40,670; David J. Kaplan, Reg. No. 41,105; Charles A. Mirho, Reg. No. 41,199; Leo V. Novakoski, Reg. No. 37,198; Naomi Obinata, Reg. No. 39,320; Thomas C. Reynolds, Reg. No. 32,488; Kenneth M. Seddon, Reg. No. 43,105; Mark Seeley, Reg. No. 32,299; Steven P. Skabrat, Reg. No. 36,279; Howard A. Skaist, Reg. No. 36,008; Steven C. Stewart, Reg. No. 33,555; Raymond J. Werner, Reg. No. 34,752; Robert G. Winkle, Reg. No. 37,474; and Charles K. Young, Reg. No. 39,435; my patent attorneys, and Thomas Raleigh Lane, Reg. No. 42,781; Calvin E. Wells, Reg. No. P43,256, Peter Lam, Reg. No. P44,855; and Gene I. Su, Reg. No. 45,140; my patent agents, of INTEL CORPORATION; and James R. Thein, Reg. No. 31,710, my patent attorney; with full power of substitution and revocation, to prosecute this application and to transact all business in the Patent and Trademark Office connected herewith.

APPENDIX B

Title 37, Code of Federal Regulations, Section 1.56 Duty to Disclose Information Material to Patentability

(a) A patent by its very nature is affected with a public interest. The public interest is best served, and the most effective patent examination occurs when, at the time an application is being examined, the Office is aware of and evaluates the teachings of all information material to patentability. Each individual associated with the filing and prosecution of a patent application has a duty of candor and good faith in dealing with the Office, which includes a duty to disclose to the Office all information known to that individual to be material to patentability as defined in this section. The duty to disclosure information exists with respect to each pending claim until the claim is cancelled or withdrawn from consideration, or the application becomes abandoned. Information material to the patentability of a claim that is cancelled or withdrawn from consideration need not be submitted if the information is not material to the patentability of any claim remaining under consideration in the application. There is no duty to submit information which is not material to the patentability of any existing claim. The duty to disclose all information known to be material to patentability is deemed to be satisfied if all information known to be material to patentability of any claim issued in a patent was cited by the Office or submitted to the Office in the manner prescribed by §§1.97(b)-(d) and 1.98. However, no patent will be granted on an application in connection with which fraud on the Office was practiced or attempted or the duty of disclosure was violated through bad faith or intentional misconduct. The Office encourages applicants to carefully examine:

(1) Prior art cited in search reports of a foreign patent office in a counterpart application, and

(2) The closest information over which individuals associated with the filing or prosecution of a patent application believe any pending claim patentably defines, to make sure that any material information contained therein is disclosed to the Office.

(b) Under this section, information is material to patentability when it is not cumulative to information already of record or being made or record in the application, and

(1) of a claim; or It establishes, by itself or in combination with other information, a prima facie case of unpatentability

(2) It refutes, or is inconsistent with, a position the applicant takes in:

(i) Opposing an argument of unpatentability relied on by the Office, or

(ii) Asserting an argument of patentability.

A prima facie case of unpatentability is established when the information compels a conclusion that a claim is unpatentable under the preponderance of evidence, burden-of-proof standard, giving each term in the claim its broadest reasonable construction consistent with the specification, and before any consideration is given to evidence which may be submitted in an attempt to establish a contrary conclusion of patentability.

(c) Individuals associated with the filing or prosecution of a patent application within the meaning of this section are:

(1) Each inventor named in the application;

(2) Each attorney or agent who prepares or prosecutes the application; and

(3) Every other person who is substantively involved in the preparation or prosecution of the application and who is associated with the inventor, with the assignee or with anyone to whom there is an obligation to assign the application.

(d) Individuals other than the attorney, agent or inventor may comply with this section by disclosing information to the attorney, agent, or inventor.